

Holistic Investigations, an Interview with Lawrence Dietz – Military and Commercial Information Security and Intelligence Expert

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining me today is Lawrence Dietz.

He has over 30 years of military and commercial information security and intelligence experience. Recent assignments have included developing the IT and legal chapters of the implementation plan for the BioPHusion Center of the CDC. Projects include intelligence fusion planning, data forensics strategic analysis.

Previous to resuming independent consulting in 2007, Dietz held key senior marketing roles at Symantec Corporation for six years. Prior to Symantec, Dietz held senior Marketing, Market Research and Customer Support Management roles. He is a licensed attorney in California and retired from the Army Reserve as a Colonel after 27 years of intelligence, PSYOP and information operations assignments. He holds Bachelor of Science in Business Administration from Northeastern University; MBA from Babson College; JD from Suffolk University; LLM in European Law from the University of Leicester in the UK, and MS in Strategic Studies from the U.S. Army War College.

Welcome to the show Larry.

Lawrence Dietz: Well, thanks Brian. Good to be here.

Brian Contos: Larry, today we are getting a bit of a departure from some of our more traditional topics to talk about something called holistic investigation. This is most likely a new concept to many of our listeners. Could you tell us what exactly this is and why do we care?

Lawrence Dietz: Well, holistic investigation actually means the marriage of traditional investigation, the kind you see in television where people are followed, dumpsters are raided, backgrounds are checked. Traditional investigation typically done by licensed private investigators like my partner Jonathan, merging that with more technologically oriented investigations that bring to their disciplines that normal private investigators don't have, sometimes data forensics and other tools. And the holistic investigation is able to address the entire environment where the inappropriate or illegal behavior maybe occurring, and is able to gather evidence that is very effective in terms of whatever remedy the client wants to see. And a remedy in this case, Brian, means purely administrative warning employees to... as an example log off from sensitive applications, or bringing a civil suit either against an employee, or a contractor, or potentially a competitor, and unfortunately sometimes

assisting the prosecutors in criminal prosecution. So, that's what the holistic investigations are.

Brian Contos: That sounds as a very broad set of skills. Is a holistic investigation generally done by a group or are there just incredible individuals out there that have skill sets in all these arenas?

Lawrence Dietz: Well, the most efficient holistic investigation to have done on a project team basis, and frankly interestingly enough some of the roles in these investigations that are covered a little bit latter on are pretty interesting because that will often determine the success. And so the roles in the investigation include a manager who is the key liaison to the client, as well as a legal representation because when you deal with data forensics you deal with things like covert video. The nuance of privacy is very, very important and depending on where the investigation is taking place there are very strict laws governing privacy. Then you need technical personnel in the IT side and on the Video side and you also probably need a data forensics type. So, the team has to be under the control of one manager working to orchestrate all the different players for the benefit of the client.

Brian Contos: Can you share with us some of the use cases, your stories from the trenches if you will, some of these holistic investigations that you have been part of?

Lawrence Dietz: Yeah. Probably the most interesting one we did was for a hospital. I call it simply Brian the case of the dirt bag doctor. And, the hospital suspected that one of their contract surgeons was inappropriately accessing patient records and sending those patient records outside of the hospital system to a friend of his who was considering litigation against the hospital. And, so this investigation actually required us to employ some covert video, data forensics, as well as just good old fashioned detective work. And it was a very interesting case because of the need to synchronize all of these different techniques and because medical information generally conceded internationally as among the most sensitive information. And I actually got them to go to the site and watch the installation of the camera and layout how the camera looks down in a doctors lounge where there are multiple computers that are connected to the hospital network.

And so the name of the game is to place the suspects on one of the video terminals there, one of either the Citrix connected terminal or the PC, and then track what was going on in that particular workstation. And, so I would have tangible evidence showing the individual and what the individual was doing. So, that was a very interesting case.

Brian Contos: So, that is really fascinating. So, you are able to combine both what you were seeing from an IT computer network perspective with what you were actually seeing physically by augmenting that with the video analytics. Is that correct?

Lawrence Dietz: Yes. And because I am sure as most of the folks listening to this podcast know, the law is always significantly behind the technology. And, so the more dramatic and easier to understand you make it for the judge or the jury, the more likely you are to get the result you want. And so, having a video of the individual makes it pretty clear that you've established that that's the person whose fingers are doing that work.

Brian Contos: Now, you've mentioned covert video a couple of times. What exactly does that mean?

Lawrence Dietz: Well, covert video means that the camera is not obvious to the people in the room. As you know around the world everybody is on camera sooner or later, Britain being very highly populated by video cameras. And you can buy little cameras that either

are very small and concealable, or you can buy cameras that are in... what looks like normal things, like motion sensors for burglar alarms, or pencil sharpeners, or a variety of other things. And the camera then is connected with an Ethernet cable to a digital video recorder and you can manage the recording and view the recording remotely. So, the investigators don't have to be on site and the environment is left pretty much intact, so nobody knows that there is any kind of video activity.

Brian Contos: So, I have to imagine that in doing this type of investigation that there are all sorts of issues, technical, political or otherwise that you run into, and some gaps and challenges that you have to address. Can you share a couple of examples of some of the barriers or roadblocks that you have come up against?

Lawrence Dietz: Well, actually one of the more interesting ones frankly is the IT chain of command. Who is in charge of what when it comes to information technology? And, so if you are going and try to manage something remotely you need to port open and you need some secure link from the outside-in. So, that means you have to have a trusted IT inside or on-site. Of course, within an investigation like this, you try and minimize the people that know to maximize the security. And so it gets interesting when an organization outsources. And, so the IT department can be actually non employees and you have to work through your client to top management to get access to the trusted IT manager on the inside there, at the location. That's kind of interesting.

Also, you have to be physically careful as to where and how the camera and the DVD are set up. And you also have to be very industrial engineering oriented if you will to set up the work flow and identify which computers are what and how the video is reviewed to cue the forensics guy as to when to look at what data stream. So, it can be pretty cool.

Brian Contos: In that you are dealing with global corporations, dealing with various countries, I know France for example has very different privacy laws than dealing with countries in the Asia-Pacific. Does that add yet another layer of complexity to this?

Lawrence Dietz: Well, not only does it add another layer of complexity, but it also adds some challenges in terms of what kind of investigators can perform this kind of role. So, we are very fortunate that we have a network of trusted contacts in most countries around the world. Because like I said my partner is a licensed private investigator. So, he has that chain, and believe it or not, there is even a group called Worldwide Association of Detectives with the unfortunate acronym of WAD.

Brian Contos: [laughs]

Lawrence Dietz: So, his connections are on that side and my connections run through the information security RSA, ISSA kind of world. So, they are very complimentary. And since I am also an attorney and have done work in international data privacy, I am pretty sensitive as to where we need to go. And frankly Brian, most of our clients that I deal with are general counsel. And so, we as the legal brains behind the operation here, pretty much retain the final authority on the privacy implications and so on. But, you are right on in terms of the legal environment. It's pretty cloudy.

Brian Contos: You know that story about that dirt bag doctor was very interesting. Do you have any other stories like that that you can share? Maybe one more?

Lawrence Dietz: Well, we have one case, I don't know how relative is to your folks, the listeners but it is kind of interesting. We had a celebrity, a young celebrity; young defined as 20s, nothing to do one night, thought she'd take some photos of her cell phone in hotel

room, and send them to her trusted boyfriend. And you will never believe this Brian, you will be totally shocked, but those photos ended up on the Internet.

Brian Contos: No way.

Lawrence Dietz: Yes. It's true. And so we had to go through the process of figuring out who had access to the photos, when were they transmitted, do we want to file a lawsuit to use the penal power to get ISPs to turnover connect records and so on and so forth. And, unfortunately, I can't give you a lot details on that one. That was pretty confidential. You get the picture so to speak.

Brian Contos: So, you really cover the spectrum from international espionage to young starlets dealing with mistakes they've made online? [laughs]

Lawrence Dietz: Well, interestingly enough, the technology connection is kind of ubiquitous in the sense that it touches the most mundane businesses or institutions as well as almost any individual traveling. I mean, all of these have a multifunctional supery duppery phone, which can be a camera. And so there is a technology aspect to a lot of this. And part of what needs to be done is, if you think there is something going wrong, whether a result of an insider or outsider effort, you have to think about the chain of events, particularly as they'll evolve through the legal system when you undertake an investigation.

Brian Contos: Larry, we have about time for you to wrap up.

Lawrence Dietz: Well, I think, it's important for organizations, particularly ones that have valuable intellectual property, trade secrets data, or are fiduciaries, meaning, they are legally responsible for other people's data. It's important to be aware of potential incidents. And the use of a combined set of techniques - traditional investigation plus technologically oriented ones can be very, very effective. So, the folks need to see who is motivated to try and penetrate or steal their information. What kinds of legal ramifications are likely to happen? And in the event that they involve sensitive data, they might want to consider the use of a firm like ours that can have international capability, legal competence, as well as the ability to apply a variety of investigative tools.

Brian Contos: You know Larry, just one very short follow-up on that. Given the economic crisis and it's been reported that the number of threats from trusted employees, partners, consultants, contractors, etc. has increased markedly. Are you getting the sense that this type of investigation, this combination of traditional, and IT, and data forensics investigation is going to become even in higher demand as people are losing jobs or fearing that they are going to lose their jobs, etc.?

Lawrence Dietz: Well, our business is certainly seeing an uptake, but perhaps more interesting we have a number of clients who are engaging in a reduction in force. And they hire us to assess the environment of how the reduction of force is going to be handled and to recommend a security and contingency procedure that can be emplaced during the actual termination process. We also provide guidance on how to minimize your exposure to former trusted insiders. And so, we have seen a growth on the preventive side, as well as some growth on the "Whoops, this is really happening" side.

Brian Contos: Well, Larry, thank you so much for joining us today on the podcast.

Lawrence Dietz: You are more than welcomed, my pleasure.

Holistic Investigations with Lawrence Dietz

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200